

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11234647 A**

(43) Date of publication of application: 27 . 08 . 99

(51) Int. Cl.

H04N 7/167

H04N 5/44

H04N 5/76

(21) Application number: **10032466**

(22) Date of filing: 16 . 02 . 98

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor: **MASUDA ISAO
GOTO YOSHIMASA
HARADA TAKENOSUKE
MACHIDA KAZUHIRO
KATAOKA MITSUTERU
NAKAMURA YASUHIRO**

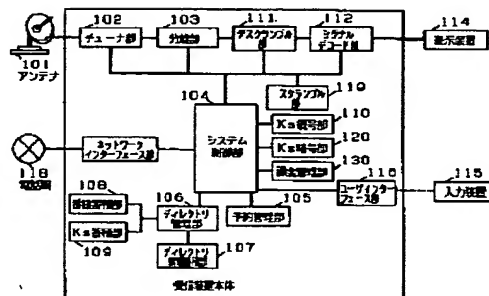
(54) STORAGE TYPE BROADCAST RECEIVER

(57) Abstract:

PROBLEM TO BE SOLVED: To ensure the security and the copyright or the like of a stored program by encrypting the program and storing the encrypted program in the storage type receiver for a broadcast system where a broadcast program is encrypted and the encrypted program is broadcast.

SOLUTION: A Ks storage section 109 and a program storage section 108 store a scramble key that is broadcast, separated and encrypted by a separate section 103, and a program encrypted by the scramble key. When viewing the stored program, a Ks decoding section 110 decodes the scramble key. A descramble section 111 descrambles the encrypted program by using a decoded scramble key and the decoded program is viewed on a display device 114. The security of the stored program is protected by storing the encrypted program in this way.

COPYRIGHT: (C)1999,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-234647

(43) 公開日 平成11年(1999) 8月27日

(51) Int.Cl.⁶

識別記号

F I

H 0 4 N 7/167
5/44
5/76

H 0 4 N 7/167
5/44
5/76

Z
A
Z

審査請求 未請求 請求項の数14 O L (全 14 頁)

(21) 出願番号

特願平10-32466

(22) 出願日

平成10年(1998) 2月16日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 増田 功

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 後藤 吉正

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 原田 武之助

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 弁理士 滝本 智之 (外 1 名)

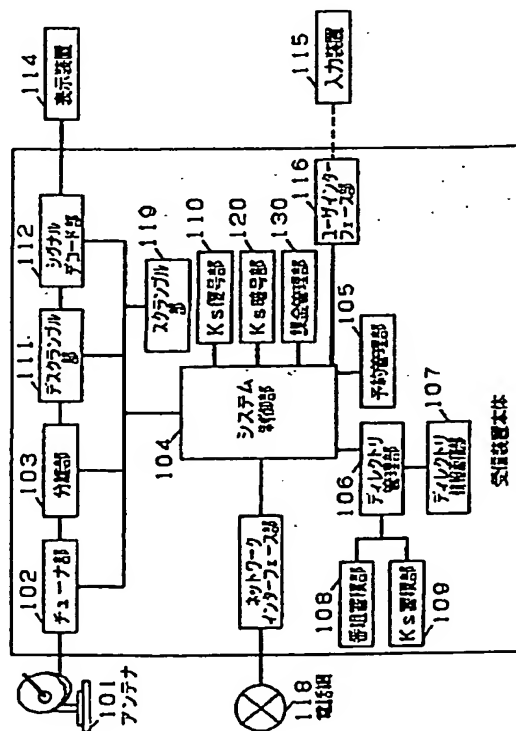
最終頁に続く

(54) 【発明の名称】 蓄積型放送受信装置

(57) 【要約】

【課題】 放送番組を暗号化して放送する放送システムの蓄積型の受信装置において、番組を暗号化して蓄積することによって、蓄積された番組の秘匿性や著作権などを保持することを目的とする。

【解決手段】 放送され、分離部103によって分離された暗号化したスクランブル鍵とそのスクランブル鍵によって暗号化した番組を、Ks蓄積部109、および番組蓄積部108に蓄積する。蓄積した番組を視聴する際にスクランブル鍵をKs復号部110において復号する。デスクランブル部111において、復号化したスクランブル鍵を使って、暗号化した番組を復号化し、表示装置114において視聴する。このように番組を暗号化して蓄積することによって、蓄積された番組の秘匿性を保護することが出来る。



【特許請求の範囲】

【請求項 1】 スクランブル鍵を用いて放送番組を暗号化し、放送番組の秘匿性を保持する放送システムの放送受信装置であって、前記スクランブル鍵を蓄積するスクランブル鍵蓄積部と、前記スクランブル鍵によって暗号化された前記放送番組を蓄積する番組蓄積部を有したことを特徴とする蓄積型放送受信装置。

【請求項 2】 前記スクランブル鍵によって暗号化された放送番組を番組蓄積部へ蓄積する時に課金することを特徴とする請求項 1 記載の蓄積型放送受信装置。

【請求項 3】 前記番組蓄積部に蓄積されている放送番組を番組蓄積部から表示する時に課金することを特徴とする請求項 1 記載の蓄積型放送受信装置。

【請求項 4】 前記放送システムからのスクランブル鍵の変更要求に基づき、スクランブル鍵蓄積部に蓄積されているスクランブル鍵を変更するスクランブル鍵更新手段を有することを特徴とする請求項 1 記載の蓄積型放送受信装置。

【請求項 5】 前記スクランブル鍵更新手段は、放送システムからのスクランブル鍵の更新要求に基づき、スクランブル鍵蓄積部に蓄積されているスクランブル鍵を更新する前に、スクランブル鍵によって暗号化され前記番組蓄積部に蓄積されている放送番組を復号化することを特徴とする請求項 4 記載の蓄積型放送受信装置。

【請求項 6】 前記スクランブル鍵更新手段は、放送システムからのスクランブル鍵の更新要求に基づき、新しいスクランブル鍵をスクランブル鍵蓄積部に追加蓄積することにより、スクランブル鍵蓄積部に複数のスクランブル鍵を蓄積することを可能にした請求項 4 記載の蓄積型放送受信装置。

【請求項 7】 前記スクランブル鍵更新手段は、放送システムからのスクランブル鍵の変更要求に基づき、スクランブル鍵蓄積部に蓄積されているスクランブル鍵を更新する前に、スクランブル鍵を用いて暗号化され番組蓄積部に蓄積されている放送番組を復号化し、新しいスクランブル鍵を用いて再度暗号化することを特徴とする請求項 4 記載の蓄積型放送受信装置。

【請求項 8】 前記番組蓄積部の暗号化された蓄積番組を検索し、蓄積した放送番組の番組一覧を作成することを特徴とする請求項 1 または請求項 4 記載の蓄積型放送受信装置。

【請求項 9】 放送番組を蓄積する番組蓄積部と、この番組蓄積部に蓄積されている前記放送番組をディレクトリ情報によって管理するディレクトリ管理部と、このディレクトリ管理部において生成される前記番組蓄積部に蓄積されている前記放送番組を管理する情報であるディレクトリ情報を前記放送システムによって放送されたディレクトリスクランブル鍵によって暗号化するディレクトリ情報暗号部と、前記ディレクトリスクランブル鍵を蓄積するディレクトリスクランブル鍵蓄積部を有した蓄

積型放送受信装置。

【請求項 10】 放送システムからのディレクトリスクランブル鍵の変更要求に基づき、ディレクトリスクランブル鍵蓄積部に蓄積されているディレクトリスクランブル鍵を変更するディレクトリスクランブル鍵更新手段を有することを特徴とする請求項 9 記載の蓄積型放送受信装置。

【請求項 11】 前記ディレクトリスクランブル鍵更新手段は、放送システムからのディレクトリスクランブル鍵の更新要求に基づき、ディレクトリスクランブル鍵蓄積部に蓄積されているディレクトリスクランブル鍵を更新する前に、ディレクトリスクランブル鍵によって暗号化され上記ディレクトリ情報蓄積部に蓄積されているディレクトリ情報を復号化することを特徴とする請求項 10 記載の蓄積型放送受信装置。

【請求項 12】 ディレクトリスクランブル鍵更新手段は、放送システムからのディレクトリスクランブル鍵の更新要求に基づき、新しいディレクトリスクランブル鍵を前記ディレクトリスクランブル鍵蓄積部に追加蓄積することにより、ディレクトリスクランブル鍵蓄積部に複数のディレクトリスクランブル鍵を蓄積可能にした請求項 10 記載の蓄積型放送受信装置。

【請求項 13】 前記ディレクトリスクランブル鍵更新手段は、放送システムからのディレクトリスクランブル鍵の変更要求に基づき、ディレクトリスクランブル鍵蓄積部に蓄積されているディレクトリスクランブル鍵を更新する前に、該ディレクトリスクランブル鍵を用いて暗号化されディレクトリ情報蓄積部に蓄積されているディレクトリ情報を復号化し、新しいディレクトリスクランブル鍵を用いて再度暗号化することを特徴とする請求項 10 記載の蓄積型放送受信装置。

【請求項 14】 前記番組蓄積部の蓄積番組を、暗号化されたディレクトリ情報から検索し、蓄積した放送番組の番組一覧を作成することを特徴とする請求項 9 または請求項 10 記載の蓄積型放送受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ディジタル放送システムにおいて蓄積装置を備え、蓄積された番組に対してアクセス制御、課金を行なうことができる蓄積型放送受信装置に関するものである。

【0002】

【従来の技術】 近年、通信技術およびデータ処理技術の発展によりオーディオ情報やビジュアル情報といったマルチメディア情報がディジタル化されて利用者に提供されるようになり、また大容量の記憶媒体の登場により大量のデータを放送し、ユーザ側の端末装置で受信、蓄積し、任意のタイミングで視聴するという放送システムが可能な状況になってきている。また、限定された視聴者のみに番組を視聴可能にする限定受信システムが、衛星

ディジタル放送において、サービスが可能になっている。図 2 1 に、現在実用化されている衛星ディジタル放送である、Perfect TV の限定受信システムの構成を示す。1 1 は、映像などの番組データである。1 2 は、映像などの番組データをスクランブルするためのスクランブル鍵である。1 3 は、スクランブル鍵を暗号化するワーク鍵である。1 4 は、送信側においてワーク鍵を暗号化するマスタ鍵である。1 5 は、受信側においてワーク鍵を復号化するマスタ鍵である。まず番組データ 1 1 を、スクランブル鍵 1 2 によって、スクランブルする (S (ステップ) 1 6)。そのスクランブル鍵 1 2 を、ワーク鍵 1 3 によって暗号化する (S 1 7)。そのワーク鍵 1 3 を、マスタ鍵 1 4 によって暗号化する (S 1 8)。暗号化されたスクランブル鍵、暗号化されたワーク鍵を、スクランブルされた番組のデータと多重する (S 1 9)。多重したデータを衛星波によって放送する (S 2 0)。多重データを受信し、受信装置において、

8 スクランブルされた番組のデータ、暗号化されたスクランブル鍵、暗号化されたワーク鍵を分離する (S 2
12 1)。暗号化されたワーク鍵を、マスタ鍵 1 5 によって
復号化する (S 2 2)。暗号化されたスクランブル鍵を、
復号化されたワーク鍵によって復号化する (S 2
13 3)。復号化されたスクランブル鍵を使って、スクラン
ブルされた番組データをデスクランブルする (S 2
4)。デスクランブルされた番組のデータを表示装置に
送り、表示する (S 2 5)。

【0 0 0 3】番組の蓄積に関しては、特開昭 6 3 - 1 0 7 2 8 1 号公報に開示した番組コピー防止技術のように、再録画防止を目的としたものがある。

【0 0 0 4】

【発明が解決しようとする課題】しかしながら、従来における番組コピー防止技術は、再録画防止を目的としたものであるため、番組をスクランブルしたまま、蓄積することができない。また、Perfect TV のシステムにおいては、番組を受信した時点で課金が行われていた。番組をスクランブルしたまま蓄積し、視聴するときにデスクランブルする手段を持たなかった。そのため、番組の秘匿性を保ったまま、視聴者が蓄積された番組を見た場合にのみ課金することが出来なかった。また、蓄積された番組のアクセス制御を行なうために用いられる暗号鍵を更新する手段を持たなかった。そのため、その暗号化鍵を破られた場合に、蓄積番組を保護するために、鍵の更新を行なう方法を持たなかった。

【0 0 0 5】

【課題を解決するための手段】この課題を解決するために、本発明は、第 1 に、スクランブルした番組を蓄積し、それを管理する情報を蓄積する手段を備えるものである。これにより、番組の秘匿性を保ちながら、番組を蓄積し、蓄積した番組の視聴が可能になる。第 2 に、端末に番組を蓄積し、それを管理するディレクトリ情報を

スクランブルして蓄積する手段を備えたものである。これにより、番組の秘匿性を保ちながら、番組を蓄積し、蓄積した番組の視聴が可能になる。

【0 0 0 6】

【発明の実施の形態】(実施の形態 1) 以下、本発明の実施の形態について、図を用いて説明する。

【0 0 0 7】図 1 は、番組を暗号化して蓄積することができる受信端末の構成図を示す。図 1 において、1 0 1 は放送波を受信するアンテナである。1 0 2 は、アンテナから受信された放送波から希望するトランスポートストリーム、TS (Transport Stream) を選択し受信するチューナ部である。TS は、MPEG 2 システム規格に準拠したトランスポート・パケットからなる。1 0 3 は、受信した TS から番組データ、番組データのスクランブルを解くスクランブル鍵、番組管理情報等を分離する分離部である。1 0 4 は、各部から各種情報を受け取り、一定処理を行ない、他の部へ情報を送り出すシステム制御部である。1 0 5 は、システム制御部 1 0 4 から予約に関する情報を受け取り、予約管理情報を生成し予約管理を行なう予約管理部である。1 0 6 は、システム制御部 1 0 4 から蓄積する番組に関する情報と、番組データやスクランブル鍵を受け取り、蓄積番組を管理するディレクトリ情報を生成し、蓄積番組を管理するディレクトリ管理部である。1 0 7 は、ディレクトリ管理部 1 0 6 からディレクトリ情報を受け取り保存するディレクトリ情報蓄積部である。1 0 8 は、ディレクトリ管理部 1 0 6 から番組データを受け取り、指定されたアドレスに蓄積する番組蓄積部である。1 0 9 は、スクランブル鍵を蓄積する K s 蓄積部である。1 1 0 は、分離部 1 0 3 から分離されたスクランブル鍵の復号化を行う K s 復号部である。1 1 1 は、分離部 1 0 3 または、システム制御部からスクランブルされた番組データを受け取り、K s 復号部からスクランブル鍵を受け取り、番組データの復号化を行なうデスクランブル部である。1 1 2 は、デスクランブル部から番組データを受け取り、表示装置 1 1 4 に表示できる形式に信号を変換するシグナルデコード部である。1 1 3 は、番組管理情報から課金情報を取り出し、課金情報を管理蓄積する課金管理部である。1 1 4 は、番組や各種情報を表示する表示装置である。1 1 5 は、ユーザの要求を受け付ける入力装置である。1 1 6 は、入力装置 1 1 5 からの入力を受け付けるユーザインタフェースである。1 1 7 は、システム制御部 1 0 4 から受け取った情報を外部ネットワーク、この場合電話網 1 1 8 に出力するネットワークインターフェース部である。1 1 8 は、外部ネットワークである電話網である。1 1 9 は、番組データの暗号化を行なうスクランブル部である。1 2 0 は、スクランブル鍵の暗号化を行なう K s 暗号部である。

【0 0 0 8】図 2 は、スクランブル鍵が配信される時の状態であるスクランブル鍵情報 3 0 1 である。スクラン

ブル鍵情報 301 は、暗号化されたスクランブル鍵本体 304 のほかに、スクランブル鍵を特定するための Ks ID (Identifier) 302 が割り当てられ、スクランブル鍵が配信された配信日 303 が付加されている。

【0009】図 3 は、番組を管理する情報である番組管理情報 401 である。番組管理情報 401 は、番組を特定するための番組 ID (Identifier) 402 と、その番組が放映されるチャンネル 403 と日時 404、その番組に対する課金情報 405、番組のタイトル 408、あらすじ等の情報が記述されている番組情報 409 からなる。また、課金情報は、サブフィールドを持ち、課金種別 406 と、課金価格 407 に別れている。

【0010】図 4 は、放送波によって配信される EPG 情報である番組プログラム管理情報 501 である。番組プログラム管理情報 501 は、現在放送されている、あるいは放送予定の番組管理情報 401 の一覧である。

【0011】図 5 は、予約管理部 105 において、番組の蓄積の予約を管理する予約管理情報 601 である。予約管理情報 601 は、予約管理識別子である予約管理 ID (Identifier) 602 と番組管理情報 401 からなる。

【0012】図 6 は、ディレクトリ管理部 106 において、蓄積番組を管理するディレクトリ情報 701 である。ディレクトリ情報は、蓄積管理 ID 702 と、番組データを蓄積する際の蓄積先頭アドレス 703、蓄積サイズ 704、番組の暗号化を行っているスクランブル鍵の Ks ID 705、番組管理情報 401 からなる。

【0013】図 7 は、視聴者が番組を予約するための番組一覧画面 801 である。図の 802 が、視聴者によって選択された番組である。

【0014】図 8 は、蓄積された番組を視聴者が選択できるようにするための蓄積番組一覧表画面 901 である。図の 902 が視聴者によって、選択された番組である。

【0015】本発明の特徴である放送番組を蓄積受信する場合の一般的な蓄積予約について説明する。放送番組や、その他情報は、放送波によって多重されて放送されている。ユーザが入力装置 115 によって番組一覧の表示を要求すると、その時受信されているトランスポートストリーム、TS (Transport Stream) から分離部 103 によって番組に関する EPG (Electric Program Guide) 情報を分離する。このシステムにおける EPG 情報は、プログラム管理情報 501 である。そのプログラム管理情報 501 をシステム制御部 104 において、ユーザが番組一覧から選択できる番組一覧画面 801 に変換し、シグナルデコード部 112 を通して、表示装置 114 に表示する。ユーザは、表示された番組一覧画面 801 から、蓄積予約したい番組を入力装置 115 によって選択する。ユーザ

が入力装置 115 によって、蓄積予約を決定すると、システム制御部 104 は、その番組管理情報 401 を取り出し、予約管理部 105 に送る。予約管理部 105 は、予約管理情報 601 を生成する。予約管理情報 601 は、予約管理部 105 において管理保存される。番組の蓄積の動作を図 9 を用いて説明する。予約管理部 105 は、常に予約管理情報 601 の番組管理情報 401 中の日時情報 404 を監視している。予約管理情報 601 の番組管理情報 401 中の日時情報 404 で、蓄積時間が来た番組について、予約管理部 105 は、システム制御部 104 に対して予約管理情報 601 の番組管理情報 401 を送り出す。システム制御部 104 は、蓄積すべきチャンネルを含む TS を受信するようチューナ部 102 に要求する。チューナ部 102 はその TS を受信する

(A1)。受信された TS は、分離部 103 において、スクランブルをかけられた番組データとスクランブル鍵情報 301 に分離される (A2)。番組データは、映像や音声のシグナルデータからなる、MPEG2 トランスポートバケットである。このバケットには、番組に使われる映像や音声データのバケットを識別するためのバケット識別子 PID (Packet Identifier) が割り当てられている。この PID は、番組が変わるときに、同時に変更される。新しいスクランブル鍵情報 301 を受信した時、そのスクランブル鍵情報 301 は、Ks 蓄積部 109 に蓄積される。分離された番組データと番組管理情報 401 は、ディレクトリ管理部 106 へ送られる。番組データは、番組蓄積部 108 において、ディレクトリ管理部 106 が指定した蓄積先頭アドレス 703 に蓄積される (A3)。番組データの終わりは、番組データに使われているデータの PID が変更されたことによって知る。番組データの終わった時点で、蓄積をやめる (A4)。ディレクトリ管理部 106 は、番組管理情報 401、蓄積されている先頭アドレス、番組データの蓄積サイズ、番組のスクランブルを行なっているスクランブル鍵の Ks ID から、ディレクトリ情報 701 を生成する (A5)。ディレクトリ情報をディレクトリ情報蓄積部 107 に蓄積する (A6)。この時、番組データはスクランブルをかけられたまま蓄積されるので、番組の秘匿性を保ったまま蓄積できる。また、ディレクトリ情報 701 は、ディレクトリ情報蓄積部 107 に保存される。蓄積された番組の視聴の一例をしめす。まず、ディレクトリ管理部 106 は、ディレクトリ情報蓄積部 107 に保存されているディレクトリ情報 701 から、必要な情報をシステム制御部 104 に送り出す。システム制御部 104 では、それら情報から、蓄積番組の一覧表画面 901 を作成する。蓄積番組一覧表画面 901 は、シグナルデコード部 112 を通して、表示装置 114 に表示される。ユーザは、その一覧から視聴したい番組を、入力装置 115 によって選択し、決定する。番組が決定されると、ディレクトリ管理部 10

6は、蓄積管理ID 702から、決定された番組を選択する。また、Ks ID 705をKs蓄積部109へ送り出し、そのKs ID 705を持つスクランブル鍵304を取り出す。そのスクランブル鍵304は、Ks復号部において、復号化される。また、システム制御部104は、選択された蓄積管理ID 702から、蓄積先頭アドレス703と蓄積サイズ704を取り出す。番組蓄積部108のそのアドレスに蓄積されている番組データを取り出し、デスクランブル部へ送る。復号化されたスクランブル鍵も、デスクランブル部へ送られ、そのスクランブル鍵を使って番組データを復号化する。復号化された番組データは、シグナルデコード部112において、表示装置114に表示できる形式にデコードされ、最終的に表示装置114に表示される。番組蓄積部108から蓄積サイズ分のデータを取り出した時点で、それらの処理を終了する。

【0016】受信装置に蓄積されている番組に対して、蓄積時に課金を行う場合の動作を説明する。

【0017】図10は、課金管理部113において管理されている課金管理情報1001である。課金管理情報1001は、番組ID 1002と課金価格1003からなる。

【0018】番組データの蓄積時に分離部103から分離された番組プログラム管理情報501の番組管理情報401をディレクトリ管理部106に送る際、システム制御部104は、番組管理情報401の課金情報405中の課金種別406で蓄積時課金が指定されているかを確認する。蓄積時課金が指定されている場合、システム制御部104は、その番組ID 402と課金情報405を課金管理部113に送る。課金管理部113は、それらの情報から、番組ID 1002とその課金価格1003を一覧にした課金管理情報1001を生成し保存する。課金管理情報1001は、定期的にネットワークインターフェース部117から電話網118を通じて放送局等の課金ホストシステムに送られる。

【0019】受信装置に蓄積されている番組に対して、視聴時に課金を行う場合の動作を説明する。蓄積された番組を視聴するとき、システム制御部104は、ディレクトリ情報701から表示画面用の情報を取り出している。その時、番組管理情報401の課金情報401中の課金種別406の中で視聴時課金が指定されているかを確認する。視聴時課金が指定されている場合、システム制御部104は、その番組ID 402と課金情報405を課金管理部113に送る。課金管理部113は、それらの情報から、番組ID 1002とその課金価格1003を一覧にした課金管理情報1001を生成し保存する。課金管理情報は、定期的にネットワークインターフェース部117から電話網118を通じて放送局等の課金ホストシステムに送られる。

【0020】スクランブル鍵更新の動作を説明する。K

sが配信されるとき、スクランブル鍵情報301として配信される。スクランブル鍵情報301は、Ks蓄積部109に保存される。放送システムからのスクランブル鍵更新要求は、新しいスクランブル鍵の配信によって行われる。新しいスクランブル鍵情報301が配信されるとき、Ks ID 302が変更されている。受信端末のシステム制御部104では、常にKs蓄積部109に保存されているスクランブル鍵情報301のKs ID 302と、受信されたスクランブル鍵情報のKs ID 302とを比較している。Ks蓄積部109に保存されているKs IDと異なるKs IDが受信されたとき、スクランブル鍵の更新が行なわれる。

【0021】Ks蓄積部109がスクランブル鍵を1つしか保存しない場合の動作の一例を、図12を用いて示す。スクランブル鍵を更新する場合、新しいスクランブル鍵情報301を放送する。システム制御部（スクランブル鍵更新手段）104では、Ks蓄積部109に蓄積されているスクランブル鍵301のKs ID 302と、受信されたスクランブル鍵のKs ID 302の比較を常に行なっている。蓄積されているKs ID 302と受信されたKs ID 302が異なる場合、スクランブル鍵の更新を受け付ける（1202）。Ks蓄積部109に蓄積されているスクランブル鍵情報301を削除する（1203）。受信されたスクランブル鍵情報301を、Ks蓄積部109に蓄積する（1204）。

【0022】さらに本発明によれば、請求項6のように、スクランブル鍵を追加蓄積する場合がある。その場合の動作の一例を、図13を用いて示す。スクランブル鍵を更新する場合、新しいスクランブル鍵情報301を放送する。システム制御部（スクランブル鍵更新手段）104では、Ks蓄積部109に蓄積されているKs ID 302と、受信されたスクランブル鍵情報301のKs ID 302の比較を常に行なっている。受信されたスクランブル鍵のKs ID 302が、蓄積されているスクランブル鍵のKs ID 502といずれも一致しなかった場合、スクランブル鍵更新を受け付ける（1302）。そして、Ks蓄積部109に空領域があるかないかを調べる（1303）。Ks蓄積部109に空領域がある場合、その空領域に受信されたスクランブル鍵情報301を保存する（1306）。Ks蓄積部109に空領域がない場合、配信日が最も古いスクランブル鍵情報301を検索する（1304）。その最も古いスクランブル鍵情報301を削除する（1305）。削除された空領域に、新しく受信されたスクランブル鍵情報301を保存する（1306）。

【0023】スクランブル鍵を更新したときに、更新前のKsで暗号化された蓄積番組を復号化して蓄積し、スクランブル鍵の更新前の番組を視聴可能にする場合の動作を説明する。この場合、Ks蓄積部109は、スクランブル鍵を1つしか保存しない。スクランブル鍵が更新

されると、システム制御部104は、更新前のスクランブル鍵情報301をKs蓄積部109から取り出す。その中のKs ID 302をディレクトリ管理部106に送る。ディレクトリ管理部106の中から、更新前のKs ID 302とディレクトリ情報701のKs ID 705と一致するディレクトリ情報701を取り出す。その情報の蓄積先頭アドレス703から番組データを番組蓄積部108から取り出す。システム制御部104は、更新前のスクランブル鍵と番組データをデスクランブル部に送り出す。デスクランブル部は、暗号化された番組データを更新前のスクランブル鍵で復号化し、復号化された番組データを、システム制御部104に送り出す。システム制御部104は、番組データ、番組情報をディレクトリ管理部106に送り出す。ディレクトリ管理部106では、新たに蓄積管理ID 702、蓄積先頭アドレス703を割り振り、Ks ID 705には何も指定せずに、ディレクトリ情報701を生成し、ディレクトリ情報蓄積部107に保存する。

【0024】このように蓄積された番組を視聴する場合の一例を示す。視聴者が視聴要求したとき、そのディレクトリ情報701のKs ID 705に何も指定がなかった場合、その番組データは、シグナルデコード部112に送られ、表示装置114に表示できる形式に変化された後、表示装置114に表示される。

【0025】スクランブル鍵を更新したときに、更新前のKsを複数個蓄積し、スクランブル鍵の更新前の番組を視聴可能にする場合の動作を説明する。スクランブル鍵が更新された場合、新しいスクランブル鍵情報301が放送される。システム制御部104では、Ks蓄積部109に蓄積されているスクランブル鍵のKs ID 302と、受信されたスクランブル鍵のKs ID 302の比較を常に行なっている。受信されたスクランブル鍵のKs ID 302が、蓄積されているスクランブル鍵のKs ID 302といずれも一致しなかった場合、Ks蓄積部109の空領域に、受信されたスクランブル鍵情報301をKs蓄積部109に保存する。Ks蓄積部109に空領域がない場合、配信日の最も古いスクランブル鍵情報が取り出され、Ks蓄積部109内のスクランブル鍵情報が削除される。システム制御部104は、取り出されたスクランブル鍵情報のKs IDをディレクトリ管理部106に送る。ディレクトリ管理部106は、ディレクトリ情報蓄積部107にあるディレクトリ情報701から、Ks IDと一致するディレクトリ情報を消去し、同時に、その情報の蓄積先頭アドレスに蓄積されている番組データを消去する。また、Ks蓄積部109のKs蓄積部109の削除された空領域に、新しく受信されたスクランブル鍵情報301を保存する。

【0026】スクランブル鍵を更新したときに、更新前のKsで暗号化された番組を復号化し、新しいスクランブル鍵で再暗号化して蓄積し、スクランブル鍵の更新前

の番組を視聴可能にする場合の動作を説明する。この場合にも、Ks蓄積部109は、スクランブル鍵を1つしか保存しない。スクランブル鍵が更新された場合、システム制御部104は、Ks蓄積部109から更新前のスクランブル鍵を取り出し、Ks復号部210へ送る。Ks復号部で復号されたスクランブル鍵は、デスクランブル部111へ送られる。更新されたスクランブル鍵も、Ks復号部110で復号化される。復号化された新しいスクランブル鍵は、スクランブル部119へ送られる。また、システム制御部104は、スクランブル鍵が更新されたことをディレクトリ管理部106に伝える。ディレクトリ管理部106では、ディレクトリ情報蓄積部107に保存されているディレクトリ情報701を参照し、更新前のKs IDを持つディレクトリ情報701と番組データを取り出し、システム制御部104へ送る。システム制御部104は、更新前の番組データをデスクランブル部111へ送り、番組データを復号化する。復号された番組データは、スクランブル部119へ送られ、新しいスクランブル鍵によって暗号化される。暗号化された番組データは、システム制御部104へ送られる。システム制御部104は、番組データと暗号を行なったスクランブル鍵のKs IDをディレクトリ管理部106へ送る。ディレクトリ管理部106は、再スクランブルされた番組データに対して、新たにディレクトリ情報701を作成する。そのとき、Ks ID 705は、暗号化を行なった更新後のスクランブル鍵のKs IDに置き換え、新たに蓄積する蓄積先頭アドレス703を記述して、作成する。番組データは、番組蓄積部208のその蓄積先頭アドレスに蓄積される。番組データの再暗号化を行なったスクランブル鍵は、Ks暗号部120に送られ、暗号化される。暗号化されたスクランブル鍵は、システム制御部104において、新しいスクランブル鍵情報301を再構成され、Ks蓄積部209に蓄積される。ディレクトリ情報701から蓄積番組用の番組一覧を作成する方法の動作を説明する。

【0027】図11は、蓄積番組用の番組一覧を表示するためにシステム制御部104において生成される蓄積番組表示情報である。1102は、蓄積番組を特定するための蓄積管理ID (Identifier)、1103は蓄積された番組のチャンネル、1104は蓄積された番組が放送された日時、1105は蓄積された番組の課金情報、1106はそのサブフィールドである課金種別、1107はその課金価格、1108は蓄積された番組のタイトル、1109は蓄積された番組の番組情報である。

【0028】まず、ディレクトリ管理部106は、ディレクトリ情報蓄積部107に保存されている蓄積管理情報701から、蓄積管理ID 702、番組管理情報401の中のチャンネル403、日時404、タイトル408、課金情報405、番組情報409を取り出し、シス

テム制御部104へ送る。これらの情報から、蓄積番組表示情報1101を生成する。蓄積番組表時情報1101の日時情報1104から、蓄積番組一覧画面801の日付、開始時間、終了時間を作り、蓄積番組表時情報のチャンネル1103から蓄積番組一覧画面のチャンネルを作り、蓄積番組表時情報のタイトル1108から、蓄積番組一覧画面のタイトルを生成し、図9の蓄積番組一覧画面を表示装置114に表示する。

【0029】（実施の形態2）デジタル放送における、蓄積番組の管理情報を暗号化して保存する受信端末の構成図を図14に示す。

【0030】図14において、201は放送波を受信するアンテナである。202は、アンテナから受信された放送波から希望するトランスポートストリーム、TS

(Transport Stream)を選択し受信するチューナ部である。TSは、MPEG2システム規格に準拠したトランスポート・パケットからなる。203は、受信したTSから番組データ、スクランブル鍵、ディレクトリスクランブル鍵、番組プログラム管理情報を分離する分離部である。204は、各部から各種情報を受け取り、一定処理を行ない、他の部へ情報を送り出すシステム制御部である。205は、システム制御部204から予約に関する情報を受け取り、予約管理情報を生成し予約管理を行なう予約管理部である。206は、システム制御部204から蓄積する番組に関する情報と、番組データやスクランブル鍵を受け取り、蓄積番組を管理するディレクトリ情報を生成し、蓄積番組を管理するディレクトリ管理部である。207は、ディレクトリ管理部206からディレクトリ情報を受け取り保存するディレクトリ情報蓄積部である。208は、ディレクトリ管理部206から番組データを受け取り、指定されたアドレスに蓄積する番組蓄積部である。209は、ディレクトリ情報701の暗号/復号化を行なうディレクトリスクランブル鍵を蓄積するKd蓄積部である。210は、分離部203から分離されたスクランブル鍵の復号化を行うKs復号部である。211は、分離部203または、システム制御部からスクランブルされた番組データを受け取り、Ks復号部からスクランブル鍵を受け取り、番組データの復号化を行なうデスクランブル部である。212は、デスクランブル部から番組データを受け取り、表示装置214に表示できる形式に信号を変換するシグナルデコード部である。213は、番組管理情報から課金情報を取り出し、課金情報を管理蓄積する課金管理部である。214は、番組や各種情報を表示する表示装置である。215は、ユーザの要求を受け付ける入力装置である。216は、入力装置215からの入力を受け付けるユーザインタフェースである。217は、システム制御部204から受け取った情報を外部ネットワーク、この場合電話網218に出力するネットワークインターフェース部である。218は、外部ネットワーク

である電話網である。219は、番組データの暗号化を行なうスクランブル部である。220は、分離部203から分離された暗号化されたディレクトリスクランブル鍵の復号化を行なうKd復号部である。221は、ディレクトリスクランブル鍵の暗号化を行なうKd暗号部である。222は、ディレクトリ情報701をディレクトリスクランブル鍵を使って暗号を行なう、ディレクトリ情報暗号部である。223は、暗号化されたディレクトリ情報701を、ディレクトリスクランブル鍵を使って復号を行なうディレクトリ情報復号部である。

【0031】図15は、ディレクトリスクランブル鍵が配信される時の状態であるディレクトリスクランブル鍵情報である。ディレクトリスクランブル鍵情報1401は、暗号化されたディレクトリスクランブル鍵本体1404のほかに、ディレクトリスクランブル鍵識別子であるKd ID (Identifier) 1402と、ディレクトリスクランブル鍵が配信された配信日1403が付加されている。

【0032】図16は、ディレクトリ管理部206によって生成される暗号化される前のディレクトリ情報1501である。ディレクトリ情報1501は、蓄積された番組データを特定するための蓄積管理ID (Identifier) 1502、番組データを蓄積する際の蓄積先頭アドレス1503、番組データの合計サイズである蓄積サイズ1504、番組管理情報401からなる。

【0033】図17は、ディレクトリ情報蓄積部207に蓄積される、暗号化された後のディレクトリ情報1601である。暗号化ディレクトリ情報1601は、ディレクトリスクランブル鍵識別子Kd ID 1602、蓄積管理ID 1603、暗号化蓄積先頭アドレス1604、暗号化蓄積サイズ1605、番組管理情報401からなる。

【0034】この場合の番組の蓄積の一例を、図18を用いて説明する。予約管理部205は、常に予約管理情報601の番組管理情報401中の日時情報404を監視している。予約管理情報401の中の日時情報404で、蓄積時間が来た番組について、予約管理部205は、システム制御部204に対して予約管理情報601の番組管理情報401を送り出す。システム制御部204は、蓄積すべきチャンネルを含むTSを受信するようチューナ部202に要求する。チューナ部202はそのTSを受信する(B1)。受信されたTSを、分離部203において、スクランブルをかけられた番組データ、スクランブル鍵情報301、ディレクトリスクランブル鍵情報1401に分離する(B2)。スクランブル鍵情報を、Ks復号部219へ送り、スクランブル鍵を復号する(B3)。受信された、またはKd蓄積部209に蓄積されているディレクトリスクランブル鍵情報1401を、Kd復号部220に送り復号する(B4)。復号化されたスクランブル鍵は、システム制御部204に戻

され、デスクランブル部211へ送られる。分離部203から分離された番組データも、デスクランブル部211へ送られる。デスクランブル部211では、復号化されたスクランブル鍵で番組データの復号化を行なう(B5)。復号化された番組データと番組管理情報401を、ディレクトリ管理部206へ送る。番組データは、番組蓄積部208において、ディレクトリ管理部106が指定した蓄積先頭アドレスに蓄積される(B6)。PIDの変更時に番組の終了を知り、蓄積を終了する(B7)。ディレクトリ管理部206は、番組管理情報401、蓄積先頭アドレス、番組データのサイズから、ディレクトリ情報1501を生成する(B8)。そしてディレクトリ管理部206は、ディレクトリ情報1501とディレクトリスクランブル鍵1404を、ディレクトリ情報暗号部222へ送る。ディレクトリ情報暗号部222は、ディレクトリスクランブル鍵を使ってディレクトリ情報1501の蓄積先頭アドレス1503、蓄積サイズ1504を暗号化する(B9)。一部暗号化したディレクトリ情報を、暗号化したディレクトリスクランブル鍵のKd IDを付加して、暗号化ディレクトリ情報1601としてディレクトリ情報蓄積部207に蓄積する(B10)。また、ディレクトリスクランブル鍵を、Kd暗号部221へ送り、暗号化する(B11)。暗号化されたディレクトリスクランブル鍵を、ディレクトリスクランブル鍵管理情報1701としてKd蓄積部209に蓄積する(B12)。この時、ディレクトリ情報の蓄積先頭アドレス1604と蓄積サイズ1605、そしてそれを復号化するディレクトリスクランブル鍵は暗号化されているので、番組の秘匿性を保つことができる。

【0035】蓄積された番組の視聴の一例を示す。まず、ディレクトリ管理部206は、ディレクトリ情報蓄積部207に保存されている暗号化ディレクトリ情報1601から、必要な情報をシステム制御部204に送り出す。システム制御部204では、それら情報から、蓄積番組の一覧表画面901を作成する。蓄積番組一覧表画面901は、シグナルデコード部212を通して、表示装置214に表示される。ユーザは、その一覧から視聴したい番組を、入力装置215によって選択し、決定する。番組を決定すると、その蓄積管理ID1603を、ディレクトリ管理部206に送る。ディレクトリ管理部206は、ディレクトリ情報蓄積部207から、その蓄積管理ID1603を持つ暗号化ディレクトリ情報1601を取り出す。そのディレクトリ情報の中のKd ID1602を、Kd蓄積部209へ送り出し、Kd蓄積部217の中から、Kd ID1402と一致するディレクトリスクランブル鍵1404を取り出す。そのディレクトリスクランブル鍵は、Kd復号部220において、復号化される。復号化されたKdとその暗号化ディレクトリ情報1601を、ディレクトリ情報復号部223に送る。ディレクトリ情報復号部223は、復号化

されたKdを使って暗号化ディレクトリ情報1601中の暗号化蓄積先頭アドレス1604と暗号化蓄積サイズ1605を復号化する。ディレクトリ情報の中の先頭アドレス1604から、番組蓄積部208のそのアドレスに蓄積されている番組データを取り出し、シグナルデコード部212へ送る。番組データを、シグナルデコード部212において、表示装置214に表示できる形式にデコードし、最終的に表示装置214に表示し、視聴できるようにする。番組は、番組蓄積部208から蓄積サイズ1605分のデータを取り出した時点で終了する。

【0036】次に、ディレクトリスクランブル鍵更新の動作を説明する。ディレクトリスクランブル鍵を配信するとき、ディレクトリスクランブル鍵情報1401として配信し、Kd蓄積部209に保存する。放送システムからのディレクトリスクランブル鍵更新要求は、新しいディレクトリスクランブル鍵の配信によって行われる。新しいディレクトリスクランブル鍵情報1401を配信するとき、Kd IDを変更している。受信端末のシステム制御部(ディレクトリスクランブル鍵更新手段)204は、常にKd蓄積部209に蓄積しているディレクトリスクランブル鍵情報のKd ID1402と、受信した鍵情報のKd ID1402とを比較している。Kd蓄積部209に保存しているKd ID1402と異なるKd IDを受信したとき、ディレクトリスクランブル鍵の更新を行なう。Kd蓄積部209がディレクトリスクランブル鍵を1つしか保存しない場合の一例を図19を用いて示す。ディレクトリスクランブル鍵を更新した場合、新しいディレクトリスクランブル鍵情報を放送する。システム制御部204は、Kd蓄積部209に蓄積されているディレクトリスクランブル鍵情報のKd ID1402と、受信されたディレクトリスクランブル鍵情報のKd ID1402の比較を常に行なっている。蓄積されているKd ID1402と受信されたKd ID1402が異なる場合、ディレクトリスクランブル鍵の更新を受け付ける(1702)。Kd蓄積部209に蓄積されているディレクトリスクランブル鍵情報を削除する(1703)。受信されたディレクトリスクランブル鍵情報1401を、Kd蓄積部209に蓄積する(1704)。

【0037】さらに本発明によれば、請求項12のように、ディレクトリスクランブル鍵を追加蓄積する場合がある。その場合の一例を、図20を用いて示す。ディレクトリスクランブル鍵が更新された場合、新しいディレクトリスクランブル鍵情報1401が放送される。システム制御部204では、Kd蓄積部209に蓄積されているディレクトリスクランブル鍵管理情報1701のKd ID1702と、受信されたディレクトリスクランブル鍵のKd ID1402の比較を常に行なっている。受信されたディレクトリスクランブル鍵のKd ID1402が、蓄積されているディレクトリスクランブル

ル鍵のKd ID 1702のいずれも一致しなかった場合、Kd更新を受け付ける(1802)。そして、Kd蓄積部209に空領域があるかないかを調べる(1803)。Kd蓄積部209に空領域がある場合、その空領域に受信されたディレクトリスクランブル鍵情報1401を保存する(1806)。ディレクトリスクランブル鍵管理情報に空領域がない場合、配信日が最も古いディレクトリスクランブル鍵情報を検索する(1804)。もっとも古いディレクトリスクランブル鍵情報を削除する(1805)。削除された空領域に、新しく受信されたディレクトリスクランブル鍵情報を保存する(1806)。

【0038】ディレクトリスクランブル鍵を更新したときに、更新前のKdで暗号化されたディレクトリ情報1601を復号化して蓄積し、ディレクトリスクランブル鍵の更新前の番組を視聴可能にする場合の動作を説明する。この場合、Kd蓄積部209は、ディレクトリスクランブル鍵を1つしか保存しない。ディレクトリスクランブル鍵を更新すると、システム制御部204は、更新前の暗号化ディレクトリ情報1601をKd蓄積部109から取り出す。その中のKd ID 1602を取り出し、ディレクトリ管理部206に送る。ディレクトリ管理部206の中から、更新前のKd ID 1602と一致する暗号化ディレクトリ情報1601を取り出し、ディレクトリ情報復号部223へ送る。また、更新前のディレクトリスクランブル鍵1404をKd復号部220へ送る。そこで、ディレクトリスクランブル鍵1404を復号し、ディレクトリ情報復号部223へ送る。ディレクトリ情報復号部223は、そのディレクトリスクランブル鍵1404を使って暗号化ディレクトリ情報1601の暗号化ディレクトリ情報1604を復号する。そして、ディレクトリ管理部206は、暗号化ディレクトリ情報のKd ID 1602に何も指定せず、暗号化蓄積先頭アドレス1604に復号化された蓄積先頭アドレスを書き込み、暗号化蓄積サイズ1605に復号化された蓄積サイズを書き込む。新たに生成された暗号化ディレクトリ情報を、ディレクトリ情報蓄積部207に保存する。

【0039】このように蓄積された番組を視聴する場合は次のようになる。視聴者が視聴要求したとき、その暗号化ディレクトリ情報のKd ID 1602に何も指定がなかった場合、そのディレクトリ情報のディレクトリ情報をそのまま参照し、番組データを番組蓄積部208から取り出す。番組データを、シグナルデコード部212に送り、表示装置214に表示できる形式変換し、表示装置214に表示する。

【0040】ディレクトリスクランブル鍵を更新したときに、更新前のディレクトリスクランブル鍵を複数個蓄積し、ディレクトリスクランブル鍵の更新前の番組を視聴可能にする場合の動作を説明する。ディレクトリスク

ランブル鍵を更新する場合、新しいディレクトリスクランブル鍵情報1401を放送する。システム制御部204では、Kd蓄積部209に蓄積されているディレクトリスクランブル鍵情報のKd ID 1402と、受信されたディレクトリスクランブル鍵情報のKd ID 1402の比較を常に行なっている。受信されたディレクトリスクランブル鍵のKd ID 1402が、蓄積されているディレクトリスクランブル鍵のKd ID 1402のいずれとも一致しなかった場合、Kd蓄積部209の空領域に、受信されたディレクトリスクランブル鍵情報1401を蓄積する。Kd蓄積部209に空領域がない場合、配信日が最も古いディレクトリスクランブル鍵情報1401を取り出し、システム制御部204へ送り、削除する。システム制御部204は、そのディレクトリスクランブル鍵情報1401をディレクトリ管理部206に送る。ディレクトリ管理部206は、ディレクトリ情報蓄積部207にあるKd IDと一致する暗号化ディレクトリ情報1601を取り出し、ディレクトリスクランブル鍵1404と共にディレクトリ情報復号部へ送り、復号化する。復号化された蓄積先頭アドレス1604と蓄積サイズ1605から、番組蓄積部のその蓄積先頭アドレスに蓄積されている番組データを消去する。そして、ディレクトリスクランブル鍵を消去する。また、Kd蓄積部209の空領域に、新しいディレクトリスクランブル鍵情報を保存する。

【0041】次にディレクトリスクランブル鍵を更新したときに、更新前のKdで暗号化されたディレクトリ情報1601を復号化し、新しいディレクトリスクランブル鍵で再暗号化して蓄積し、ディレクトリスクランブル鍵の更新前の番組を視聴可能にする場合の動作を説明する。この場合にも、Kd蓄積部109は、ディレクトリスクランブル鍵を1つしか保存しない。ディレクトリスクランブル鍵を更新する。

【0042】場合、システム制御部204は、Kd蓄積部209から更新前のディレクトリスクランブル鍵を取り出し、Kd復号部209へ送る。Kd復号部でディレクトリスクランブル鍵を復号し、ディレクトリ情報復号部223へ送る。ディレクトリ情報復号部223は、ディレクトリ情報蓄積部207から、暗号化ディレクトリ情報1601を取り出し、その中の暗号化蓄積先頭アドレス1604と暗号化蓄積サイズ1605をディレクトリスクランブル鍵1404を使って復号する。また、更新された新しいディレクトリスクランブル鍵もKd復号部220において復号化し、ディレクトリ情報暗号部222に送る。先程復号化された蓄積先頭アドレス1604と蓄積サイズ1605を、ディレクトリ情報暗号部222へ送り、新しい鍵によって暗号化する。ディレクトリ管理部206において、再暗号化された蓄積先頭アドレス1604と蓄積サイズ1605から、暗号化ディレクトリ情報1601を再構成する。この時、Kd ID

1602には、暗号化を行なった新しいディレクトリスクランブル鍵のKd IDを指定する。暗号化ディレクトリ情報1601を、ディレクトリ情報蓄積部207に蓄積する。

【0043】次に、ディレクトリ情報から蓄積番組用の番組一覧を作成する方法の動作を説明する。まず、ディレクトリ管理部206は、ディレクトリ情報蓄積部207に保存されている暗号化蓄積管理情報1601の蓄積管理ID 1602、番組管理情報401の中に記述されているチャンネル403、日時404、タイトル408、課金情報405、番組情報409を取り出し、システム制御部204へ送る。これらの情報から、蓄積番組表示情報1101を生成する。蓄積番組表示情報1101の日時1104から、蓄積番組一覧画面901の日付、開始時間、終了時間を作り、蓄積番組表示情報のチャンネル1103から蓄積番組一覧画面のチャンネルを作り、蓄積番組表示情報のタイトル1108から、蓄積番組一覧画面のタイトルを生成し、蓄積番組一覧画面901を表示装置214に表示する。

【0044】以上より、ディレクトリスクランブル鍵を暗号化すれば、これは蓄積された番組データのアドレス管理を行っているため、蓄積された番組のおのをおの暗号化せずにすむので、スクランブル処理がより早くなる。

【0045】

【発明の効果】本発明によれば、有料放送の番組を蓄積する場合に、暗号化されて放送された番組をそのまま蓄積し、その暗号を解くためのスクランブル鍵を暗号化して蓄積することにより、蓄積された番組の秘匿性を保護することが出来、蓄積された番組の視聴時に課金を行うことが出来る。番組の暗号化を行うスクランブル鍵を解読され、番組の秘匿性を破られた場合に、スクランブル鍵を新たに更新することによって、番組の秘匿性を回復することが出来る。

【0046】また、番組を蓄積する場合に、番組を復号化して蓄積するが、そのディレクトリ情報をその情報を暗号化するためのディレクトリスクランブル鍵で暗号化することによって、蓄積された番組の読み込みを不可能にし、番組の秘匿性を保護することが出来る。また、ディレクトリスクランブル鍵を放送波にのせて更新することによって、ディレクトリスクランブル鍵を破られた場合の対処を行うことが出来る。また、番組のジャンル毎にディレクトリスクランブル鍵を変更して暗号化を行うことによって、蓄積された番組をジャンル毎に管理することが出来る。

【図面の簡単な説明】

【図1】本発明における番組を蓄積する際、暗号化した番組を蓄積し、視聴する際に番組の復号化を行なう蓄積型受信装置の内部構成を示すブロック図

【図2】番組の暗号化を行なうスクランブル鍵が配信されるとき状態であるスクランブル鍵情報のフレーム図

【図3】番組を管理する情報である番組管理情報のフレーム図

【図4】放送波によって配信されるEPG情報である番組プログラム管理情報を示す説明図

【図5】番組の蓄積の予約を管理する予約管理情報のフレーム図

【図6】蓄積番組を管理するディレクトリ情報のフレーム図

【図7】番組を予約するための番組一覧画面を示す説明図

【図8】蓄積された番組を選択するための蓄積番組一覧表示画面を示す説明図

【図9】図1の受信装置における、番組の蓄積動作を示すフロー図

【図10】課金管理部によって管理されている課金管理情報を示す説明図

【図11】蓄積番組用の番組一覧を表示するためにシステム制御部において生成される蓄積番組表示情報を示す説明図

【図12】図1の受信装置における、スクランブル鍵を1つしか保存しない場合のスクランブル鍵の更新の動作を示すフロー図

【図13】図1の受信装置における、スクランブル鍵を複数保存する場合のスクランブル鍵更新の動作を示すフロー図

【図14】本発明の番組を蓄積する際、ディレクトリ情報を暗号化して番組を蓄積する積型受信装置の内部構成を示すブロック図

【図15】放送波によってディレクトリスクランブル鍵が配信されるとき状態であるディレクトリスクランブル鍵情報のフレーム図

【図16】ディレクトリ管理部によって生成される暗号化される前のディレクトリ情報のフレーム図

【図17】ディレクトリ情報蓄積部に蓄積される、暗号化された後のディレクトリ情報のフレーム図

【図18】図14の受信装置における、ディレクトリ情報を暗号化して番組を蓄積する場合のフロー図

【図19】図2の受信装置における、番組の蓄積動作を示すフロー図

【図20】図2の受信装置における、ディレクトリスクランブル鍵を1つしか保存しない場合のディレクトリスクランブル鍵更新の動作を示すフロー図

【図21】図2の受信装置における、ディレクトリスクランブル鍵を複数保存する場合のディレクトリスクランブル鍵更新の動作を示すフロー図

【符号の説明】

104 システム制御部

108 番組蓄積部

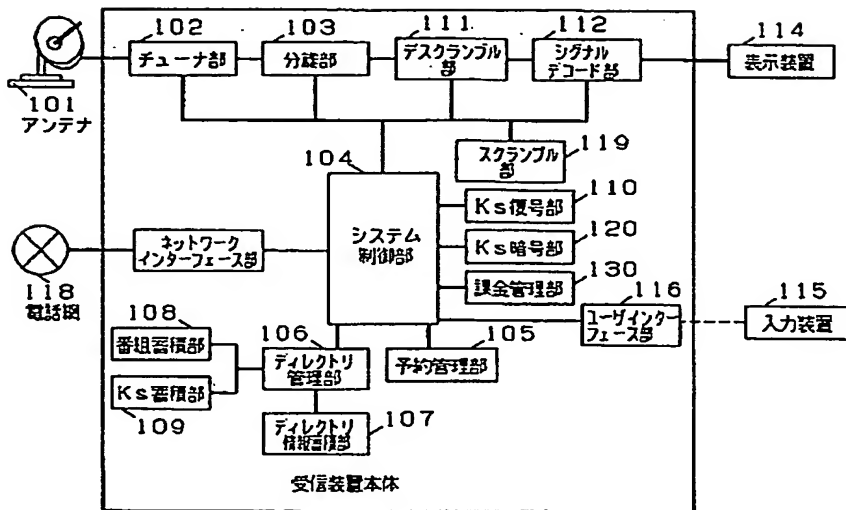
109 Ks蓄積部(スクランブル鍵蓄積部)

204 システム制御部

206 ディレクトリ管理部
208 番組蓄積部

222 ディレクトリ情報暗号部

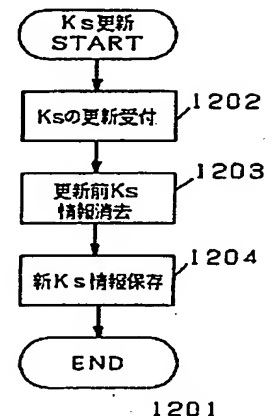
【図 1】



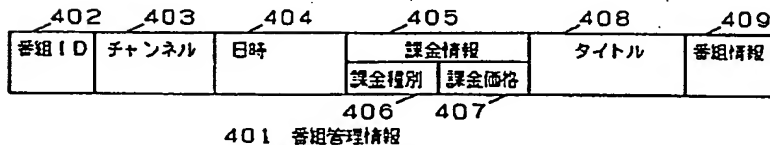
【図2】



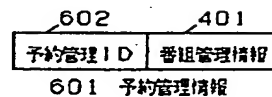
【图 12】



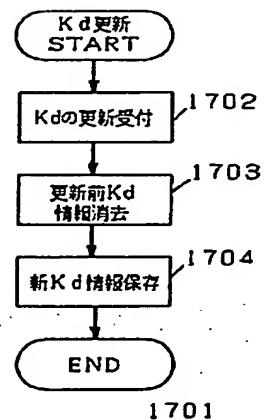
【図 3】



【図5】



【图 19】



【図4】

番組ID	チャンネル	日時	課金情報		タイトル	番組情報
			課金種別	課金価格		
0	Channel 1	10/24 19:00-20:00	番組時	¥300	ニュース	...
1	Channel 2	10/24 19:00-19:30		¥0	ニュース	...
...
n	Channel 1	10/24 21:00-23:00	視聴時	¥400	映画「東京物語2」	-

501 番組プログラム管理情報

【図 10】

1002	1003
番組ID	課金価格
5	¥450
14	¥200
...	...
n	...

1001 課金管理情報

1001 課金管理情報

【图6】

702	703	704	705	401
番組管理ID	番組先頭アドレス	番組サイズ	KsID	番組管理情報

701ディレクトリ情報

701 ディレクトリ情報

【图8】

番号	日付	開始時間	終了時間	チャンネル	タイトル
1	10/16	21:00	23:00	Channel 5	映画「こころのつたえ」
2	10/16	23:30	2:30	Channel 5	映画「こころのつたえ」
...
n	10/30	15:00	16:00	Channel 7	三宅邦子組

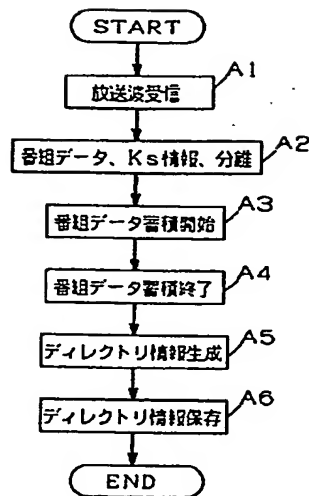
901 香頌普坦一頁表背面

【図7】

10/24	Channel 1	Channel 2	Channel 4
↑				
19時	ニュース	ニュース		野球中継
20時	バラエティ	ボクシング中継	
21時	ドラマ	映画「東京物語2」		ドラマ
22時	ドキュメント			バラエティ
↓				

801 番組一覧画面

【図9】



【図15】

1402	1403	1404
KdID	配信日	Kd

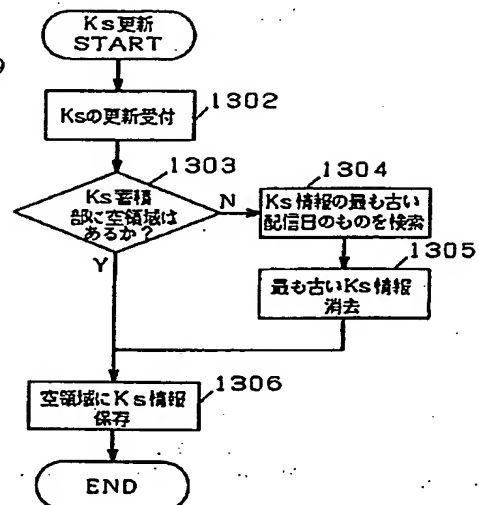
1401ディレクトリスクランブル鍵情報

【図11】

1102	1103	1104	1105	1106	1107	1108	1109
番組管理ID	チャンネル	日時	課金情報	課金種別	課金価格	タイトル	番組情報
1	Channel 5	10/16 21:00-23:00	視聴時		¥450	映画「ここより過去に」	...
2	Channel 2	10/24 19:30-21:00	蓄積時		¥200	ボクシング中継	...
...
n	Channel 7	10/30 15:00-16:00			¥0		

1101 蓄積番組表示情報

【図13】



1301

【図16】

1502	1503	1504	401
番組管理ID	蓄積先頭アドレス	蓄積サイズ	番組管理情報

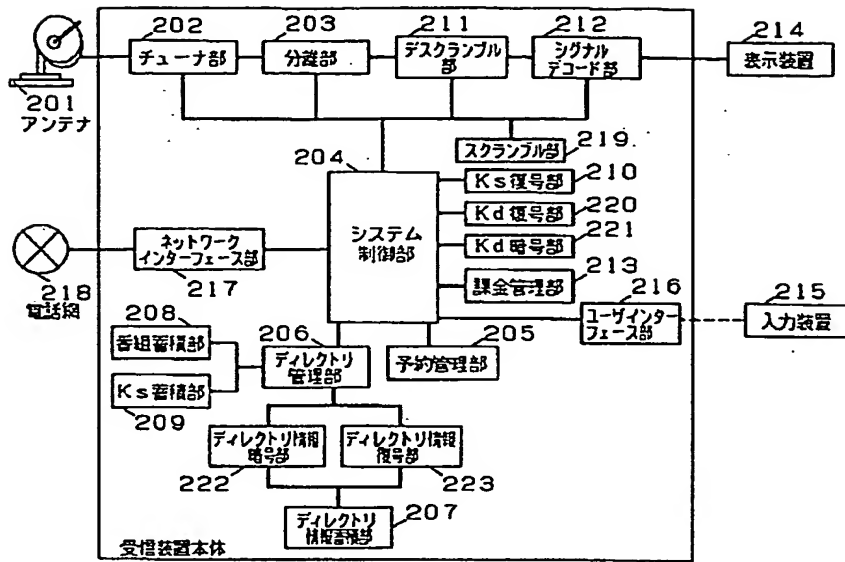
1501 ディレクトリ情報

【図17】

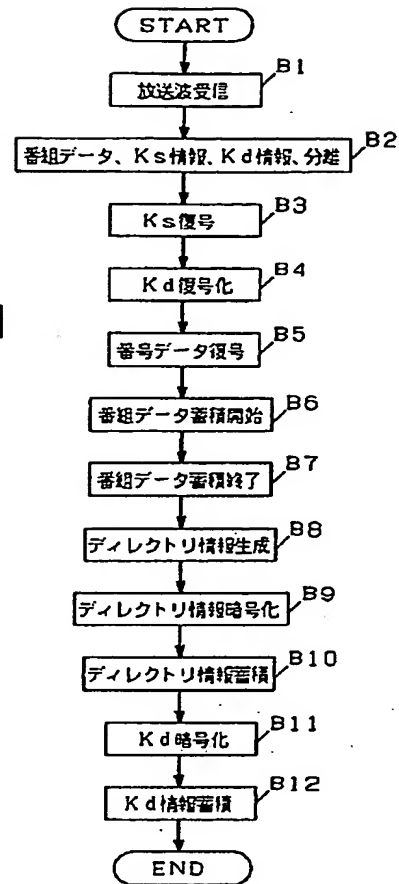
1602	1603	1604	605	401
KdID	番組管理ID	暗号化蓄積先頭アドレス	暗号化蓄積サイズ	番組管理情報

1601 暗号化ディレクトリ情報

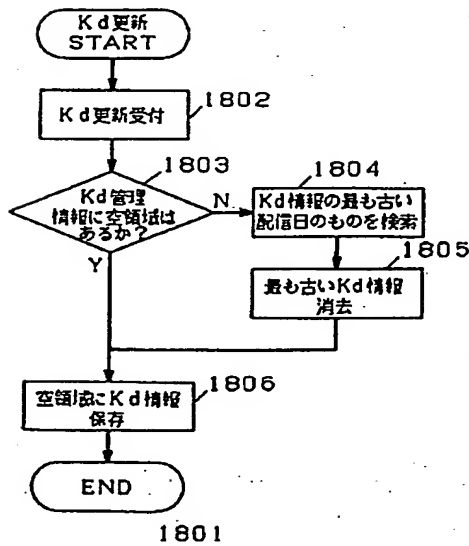
【図 1 4】



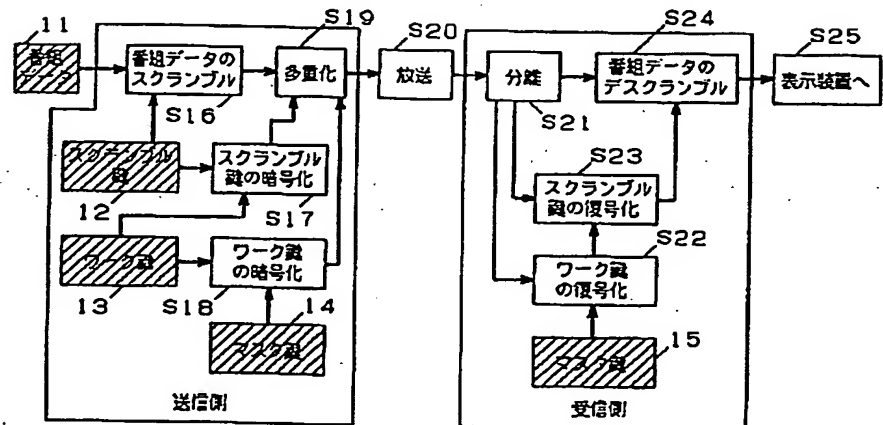
【図 1 8】



【図 2 0】



【図 2 1】



フロントページの続き

(72) 発明者 町田 和弘
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 片岡 充照
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 中村 康浩

大阪府門真市大字門真1006番地 松下電器
産業株式会社内